# 消息认证

2020年4月9日 9:54

1. 哈希函数性质
    a. 变长输入，定长输出
    b. 易计算
    c. 单向性：难求原文
    d. 抗弱碰撞：给定原文，难找同摘要的其他输入
    e. 抗强碰撞：难以找任意两个输入有相同输出
2. 哈希攻击
    a. preimage attack预映射攻击：给摘要找明文
    b. second preimage attack次预映射攻击：给明文找弱碰撞
    c. collision attack碰撞攻击：找强碰撞